Cryptography and Network Security II

Second Course

Lecture 7: Wireless Network Security

Wireless Security Overview

- Concerns for wireless security are similar to those found in a wired environment
- Security requirements are the same:
  - Confidentiality, integrity, availability, authenticity, accountability
  - Most significant source of risk is the underlying communications medium

Wireless Network Modes

- The 802.11 wireless networks operate in two basic modes:
  - Infrastructure mode
  - Ad-hoc mode
- Infrastructure mode
  - Each wireless client connects directly to a central device called Access Point (AP)
  - No direct connection between wireless clients
  - AP acts as a wireless hub that performs the connections and handles them between wireless clients

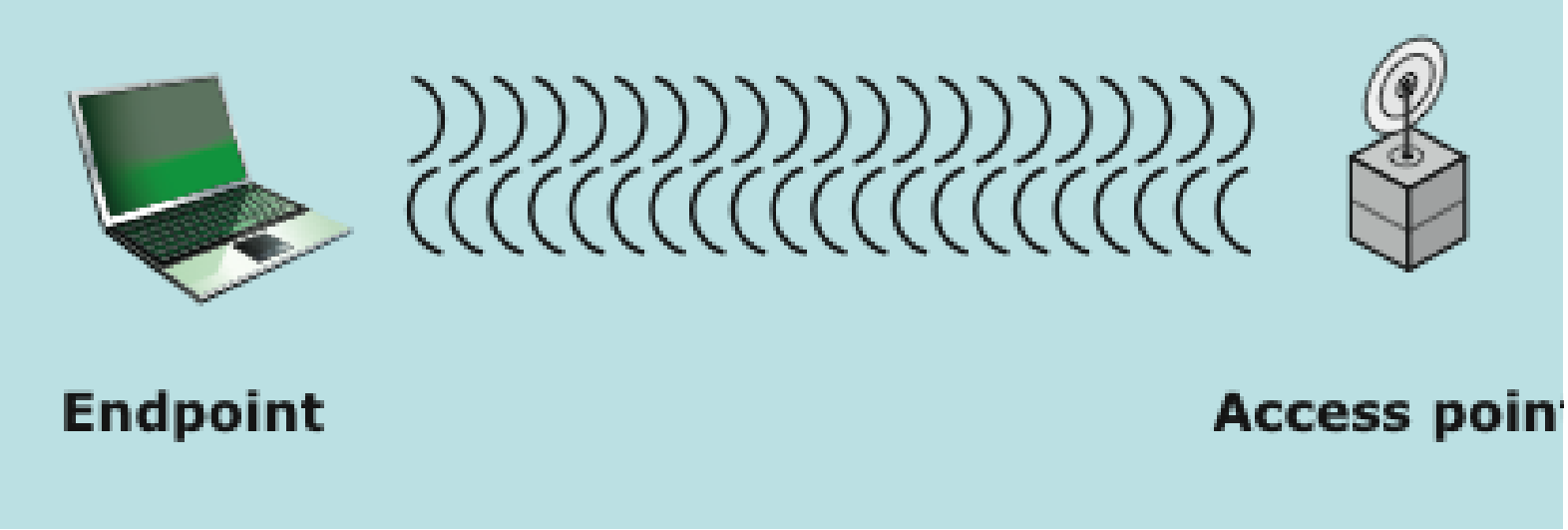
Wireless Network Modes

- Ad-hoc mode:
  - Each wireless client connects directly with each other
  - No central device managing the connections
  - Rapid deployment of a temporal network where no infrastructures exist (advantage in case of disaster…)
  - Each node must maintain its proper authentication list

Key Factors Contributing to Risks

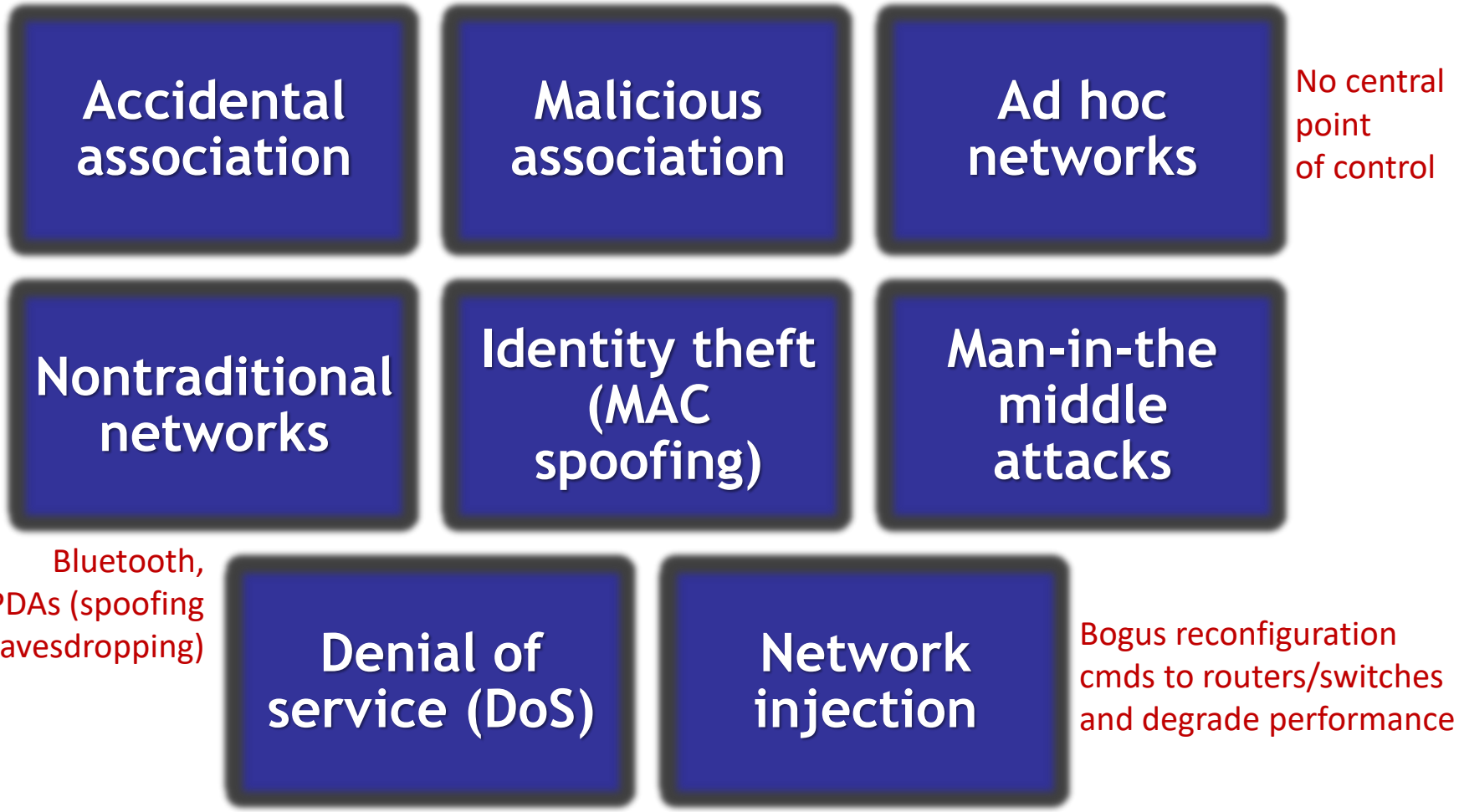
- Channel: broadcast communication (more susceptible to eavesdropping and jamming)
- Mobility: additional risks (later)
- Resources: advanced OS (iPhone, Android), but limited resources (memory, processing)
- Accessibility: Certain devices may be left unattended

Wireless Networking Components
(Facilitating points of attack)



Wireless client: WIFI-enabled laptop/tablet, cell phone, Bluetooth device, …
Access point: Cell towers, WIFI hotspots, wireless routers
Transmission medium: carries signals

Wireless Network Threats



Wireless Security Measures

- Signal hiding
  - Turn off SSID name broadcasting
  - Cryptic names
  - Reduce signal strengths (place away from windows and external walls
  - Directional antennas
- Encryption (standard)

Securing Wireless Networks

- Use encryption
- Use and enable anti-virus, anti-spyware, firewall
- Turn off SSID broadcasting
- Change default identifier on router
- Change router's preset password
- Apply MAC-filtering

SSID – Service Set Identification

- Identifies a particular wireless network
- A client must set the same SSID as the one in that particular AP Point to join the network
- Without SSID, the client won't be able to select and join a wireless network
- Hiding SSID is not a security measure because the wireless network in this case is not invisible
- It can be defeated by intruders by sniffing it from any probe signal containing it.

SSID

- A way for vendors to make more money
- It is easy to find the ID for a “hidden” network because the beacon broadcasting cannot be turned off
- Simply use a utility to show all the current networks:
  - inSSIDer
  - NetStumbler
  - Kismet

Mobile Device Security Challenges

- No more tight control over computing devices
- Growing use of mobile (endpoint) devices
- Cloud-based applications readily available (Box, Dropbox, Skype, …)
- De-perimeterization: static network perimeter is gone
- External business requirements (guests, third-party contractors, …)
- Bring Your Own Device (BYOD)
- *The above results in threats* (next page)

Mobile Device Security Threats

- Lack of physical security control
- Use of untrusted mobile devices
- Use of untrusted networks
- Use of apps created by unknown parties
- Interaction with other systems (e.g., cloud-based data sync)
- Use of untrusted contents

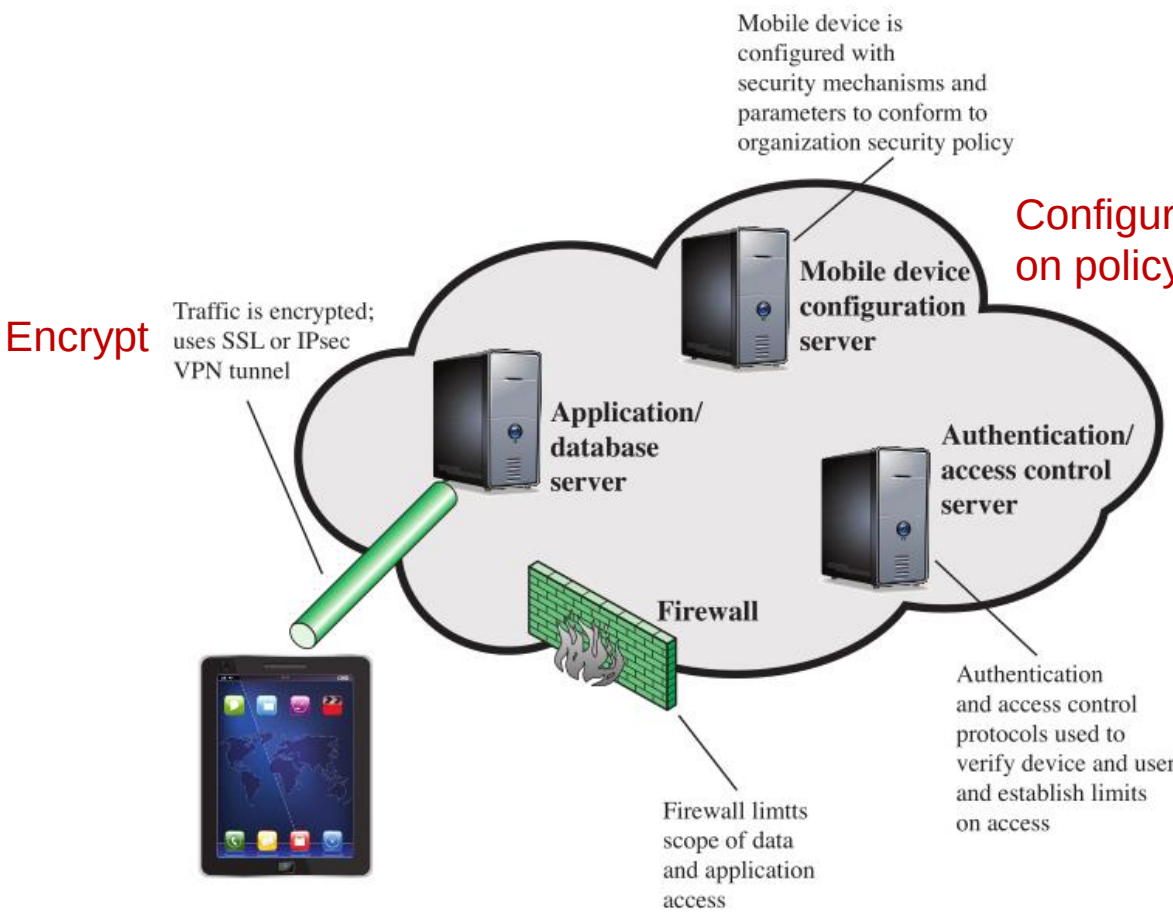
Mobile Device Security Strategy

- Device security (next slide)
- Traffic security (e.g., SSL, VPNs)
- Barrier security (e.g., firewalls, IDS/IPS)

Mobile Device Security

- Configure (enable) auto-lock
- Configure/enable SSL
- Enable password/PIN protection
- Configure (disable/discourage) auto-completion (for passwords)
- Enable remove wipe
- Up-to-date OS/software
- Install anti-virus software
- Encrypt sensitive data on mobile devices
- Prohibit installation of third-party apps
- Policy development followed by training

Mobile Device Security Elements

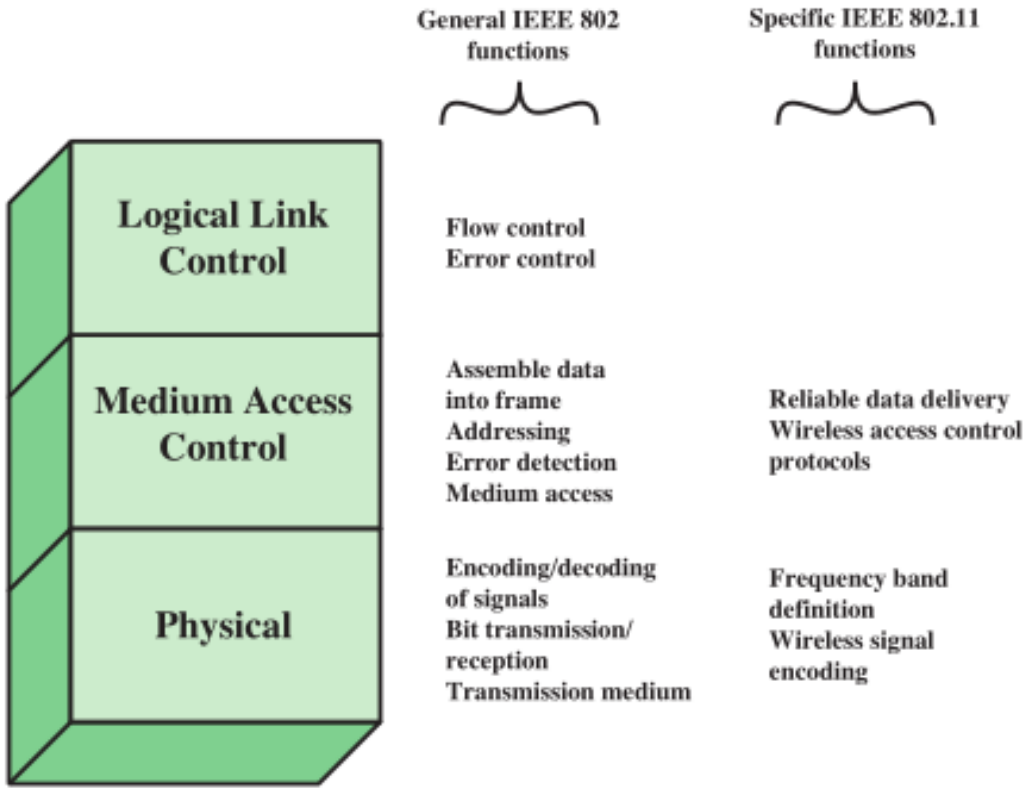


IEEE 802.11 Wireless LAN

- IEEE 802: a committee responsible for LANs
- IEEE 802.11: responsible for developing wireless protocols
  - Many standards
- The Wi-Fi alliance: became popular with 802.11b
  - Wi-Fi Protected Access (WPA, WPA2)

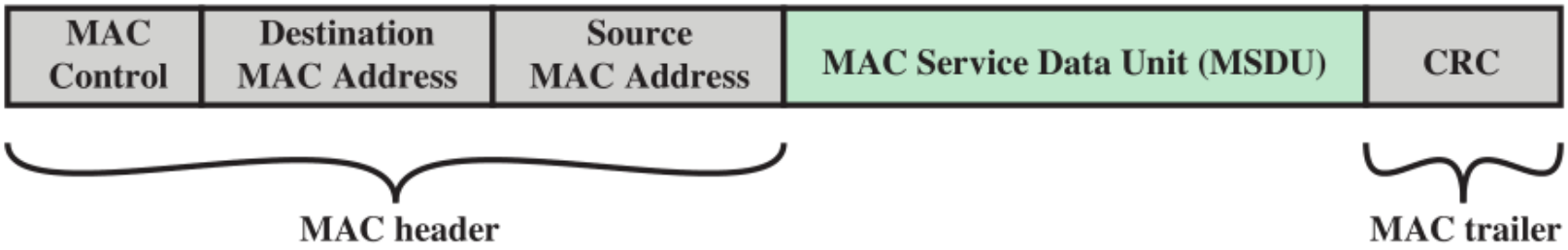
IEEE 802.11 Protocol Stack

- **Physical layer** (encode/decode signals)
- **MAC layer**: assembles MAC frame, disassembles frames and performs address recognition
- **LLC**: keeps track of frame transmission



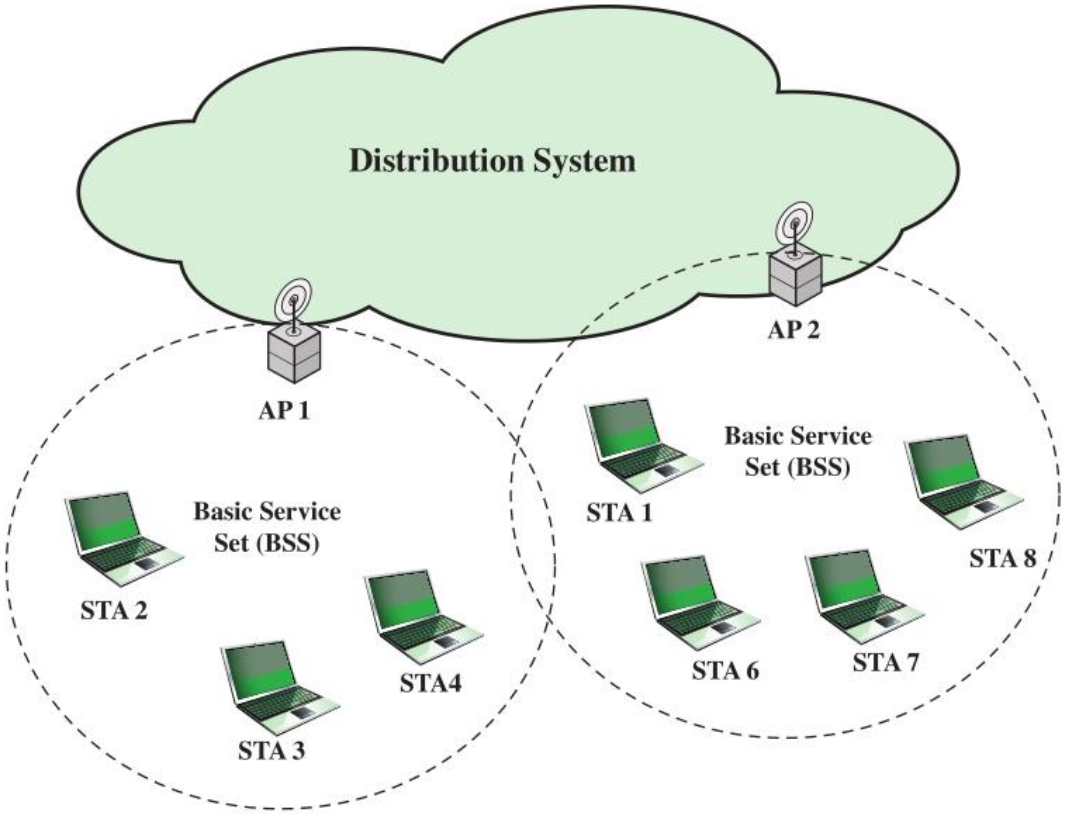
A MAC Frame (MPUD)

- MAC protocol data unit (MPUD)



IEEE 802.11 Extended Service Set

- **BSS**: the smallest building block
- BSSs connecte via **APs**
  - Aps functions as bridges
- **ESS**: two or more BSSs



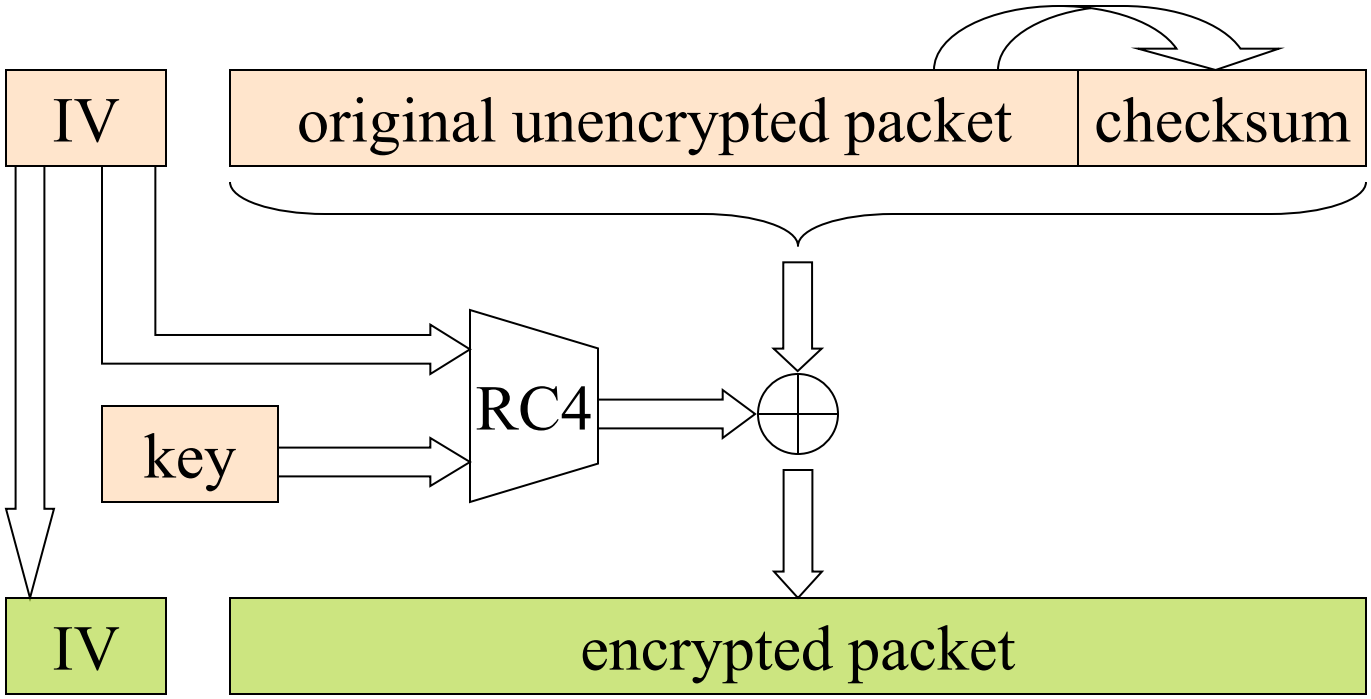
IEEE 802.11# Wireless Security

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- WPA2
- Robust Security network (RSN)

WEP - Wired Equivalent Privacy

- The original native security mechanism for WLAN
- provide security through a 802.11 network
- Used to protect wireless communication from eavesdropping (confidentiality)
- Prevent unauthorized access to a wireless network (access control)
- Prevent tampering with transmitted messages
- Provide users with the equivalent level of privacy inbuilt in wireless networks.

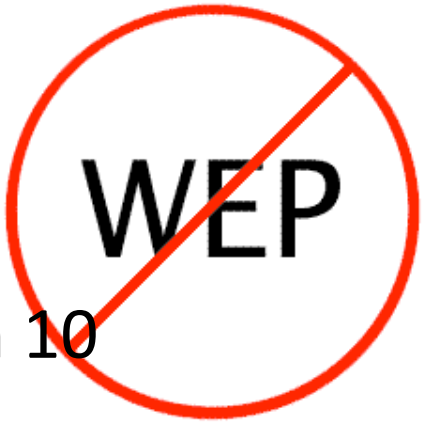
How WEP works



WEP Flaws and Vulnerabilities

- Weak keys:
  - ✓ It allows an attacker to discover the default key being used by the Access Point and client stations
  - ✓ This enables an attacker to decrypt all messages being sent over the encrypted channel.
- IV (initialization vector) reuse and small size:
  - ✓ There are 2^{24} different IVs
  - ✓ On a busy network, the IV will surely be reused, if the default key has not been changed and the original message can be retrieved relatively easily.

Attacks on WEP

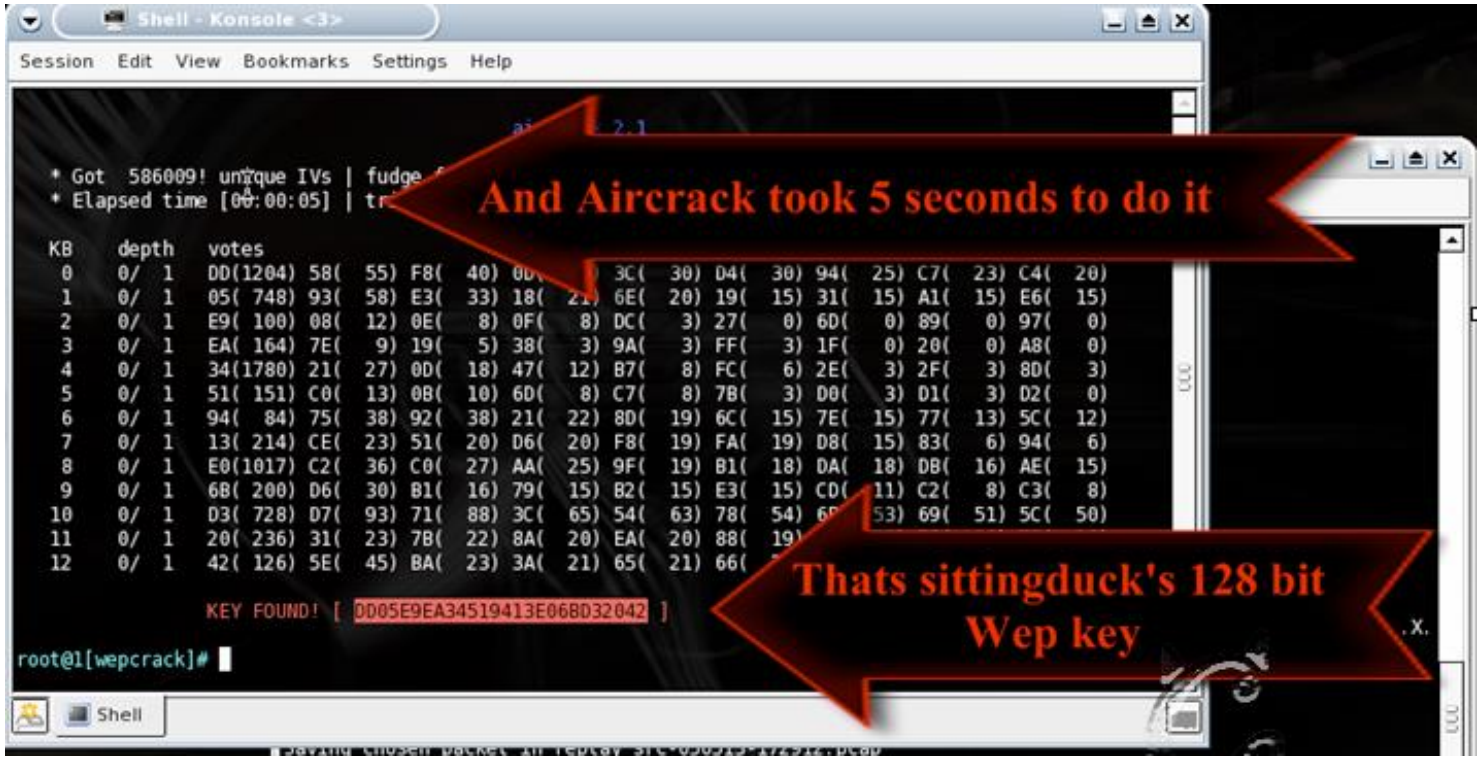


- WEP encrypted networks can be cracked in 10 minutes
- Goal is to collect enough IVs to be able to crack the key
- IV = Initialization Vector, plaintext appended to the key to avoid Repetition
- Injecting packets generates IVs

Attacks on WEP

- Backtrack 5 (Released 1st March 2012)
- Tutorial is available
- All required tools on a Linux bootable CD + laptop + wireless card

WEP Cracking Example



WPA - WI-FI Protected Access

- New technique in 2002
- Replacement of security flaws of WEP
- Improved data encryption
- Strong user authentication
- Because of many attacks related to static key, WPA minimize shared secret key in accordance with the frame transmission
- Use the RC4 algorithm in a proper way and provide fast transfer of the data before someone can decrypt the data.

WPA2 - WI-FI Protected Access 2

- Based on the IEEE 802.i standard
- 2 versions: Personal & Enterprise
- The primary enhancement over WPA is the use of the AES (Advanced Encryption Standard) algorithm
- The encryption in WPA2 is done by utilizing either AES or TKIP
- The Personal mode uses a PSK (Pre-shared key) & does not require a separate authentication of users
- The enterprise mode requires the users to be separately authenticated by using the EAP protocol

WPA2

- WPA2 has immunity against many types of hacker attacks
  - ✓ Man-in-the middle
  - ✓ Authentication forging
  - ✓ Replay
  - ✓ Key collision
  - ✓ Weak keys
  - ✓ Packet forging
  - ✓ Dictionary attacks

WEP vs WPA vs WPA2

	WEP	WPA	WPA2
ENCRYPTION	RC4	RC4	AES
KEY ROTATION	NONE	Dynamic Session Keys	Dynamic Session Keys
KEY DISTRIBUTION	Manually typed into each device	Automatic distribution available	Automatic distribution available
AUTHENTICATION	Uses WEP key as Authentication	Can use 802.1x & EAP	Can use 802.1x & EAP

Procedures to Improve Wireless Security

- Use wireless intrusion prevention system (WIPS)
- Enable WPA-PSK
- Use a good passphrase (https://grc.com/password)
- Use WPA2 where possible
- AES is more secure, use TKIP for better performance
- Change your SSID every so often
- Wireless network users should use or upgrade their network to the latest security standard released

Wireless Network Tools

- MAC Spoofing
  - http://aspoof.sourceforge.net/
  - http://www.gorlani.com/publicprj/macmakeup/macmakeup.asp
  - http://www.klcconsulting.net/smac/
- WEP Cracking tools
  - http://www.backtrack-linux.org/
  - http://www.remote-exploit.org/articles/backtrack/index.html
  - http://wepattack.sourceforge.net/
  - http://wepcrack.sourceforge.net/
- Wireless Analysers
  - http://www.kismetwireless.net/
  - http://www.netstumbler.com/

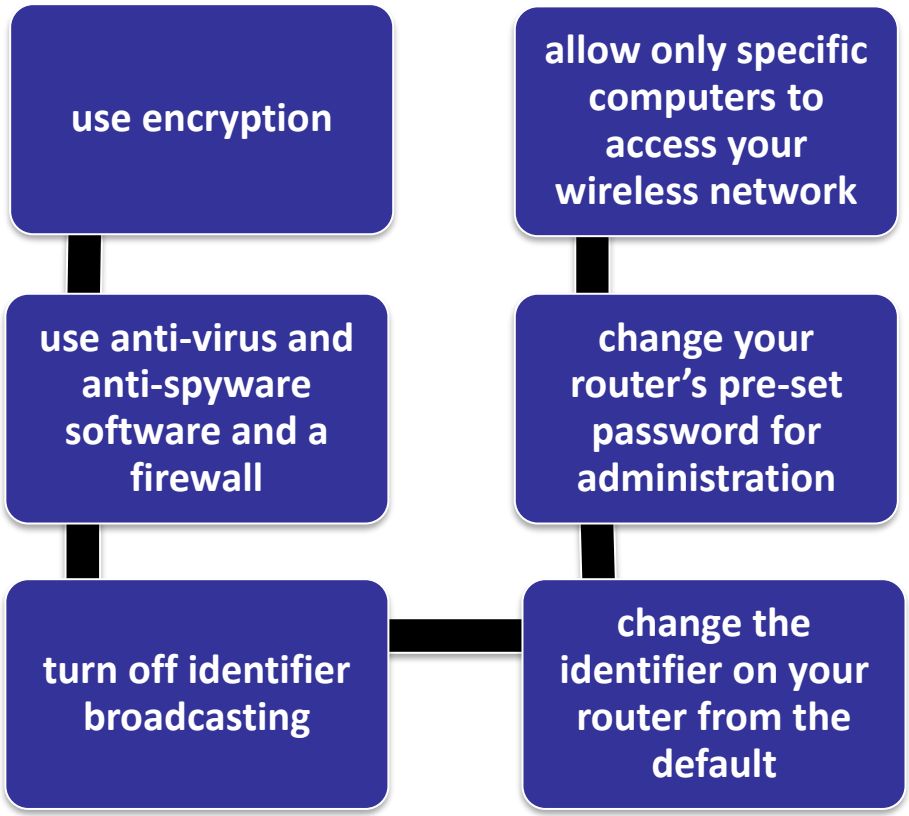
Securing Wireless Transmission

- Signal hiding (and SSID hiding)
  - Reduce signal strengths
- Encryption: encrypt all wireless transmissions

Securing Access Point

- Disallow unauthorized access to the AP
- Require authentication for any access including for devices wishing to attach themselves to the AP

Securing Wireless Networks



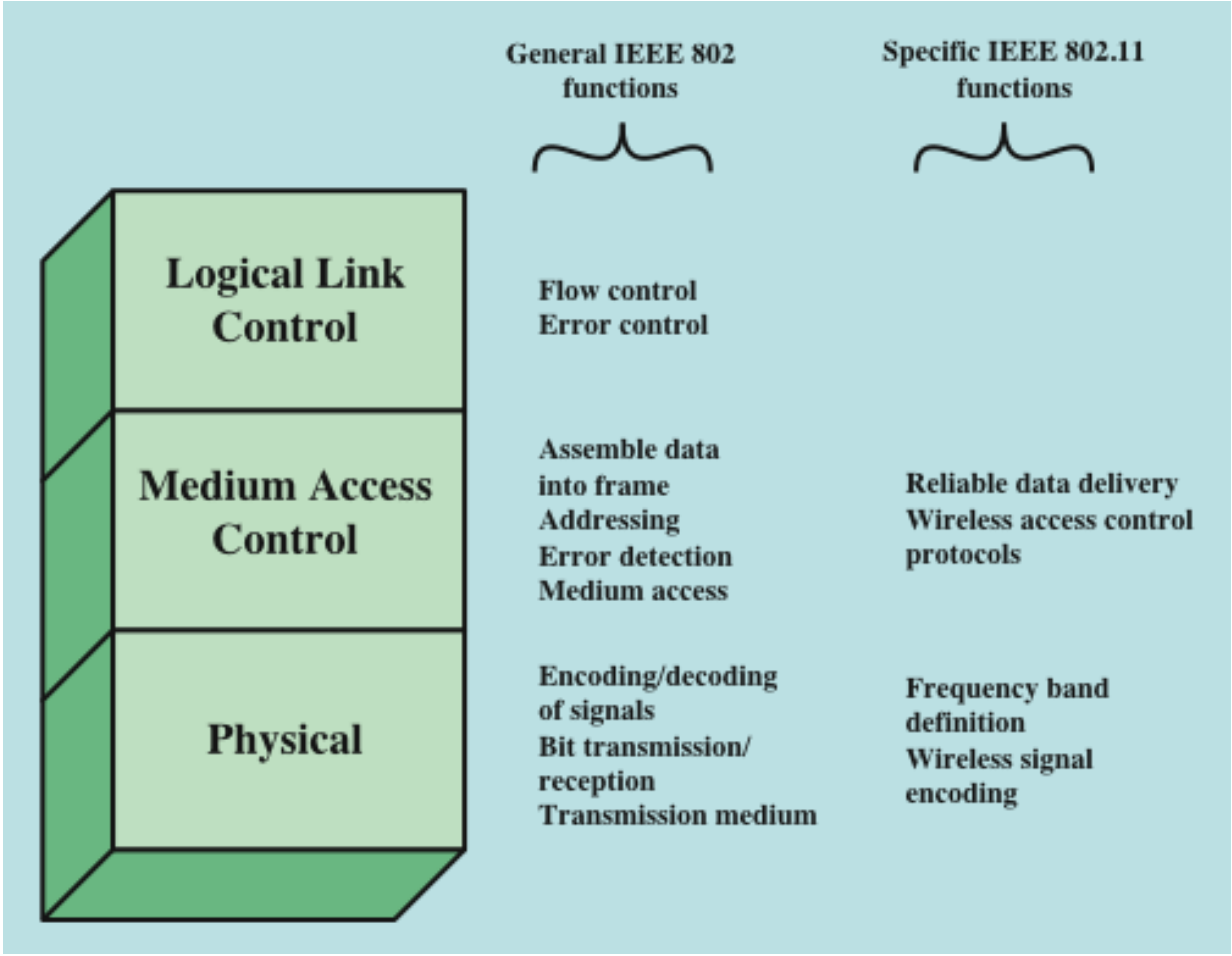
IEEE 802.11 Terminology

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

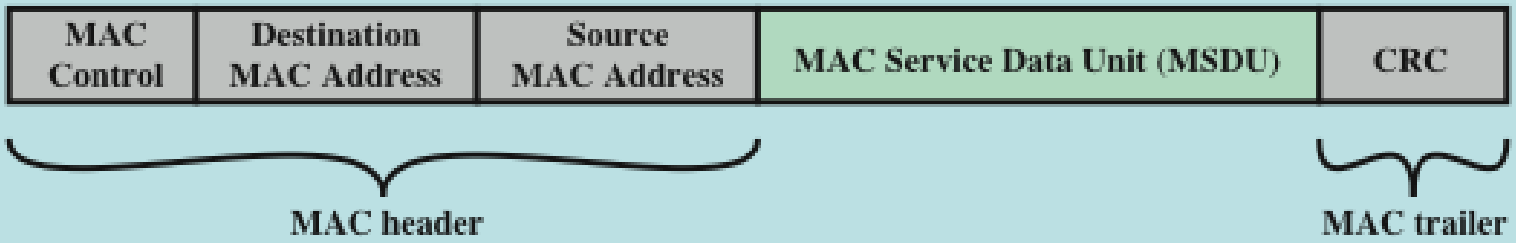
Wireless Fidelity (Wi-Fi) Alliance

- 802.11b
  - first 802.11 standard to gain broad industry acceptance
- Wireless Ethernet Compatibility Alliance (WECA)
  - industry consortium formed in 1999 to address the concern of products from different vendors successfully interoperating
  - later renamed the Wi-Fi Alliance
- term used for certified 802.11b products is *Wi-Fi*
  - has been extended to 802.11g products
- Wi-Fi Protected Access (WPA)
  - Wi-Fi Alliance certification procedures for IEEE802.11 security standards
  - WPA2 incorporates all of the features of the IEEE802.11i WLAN security specification

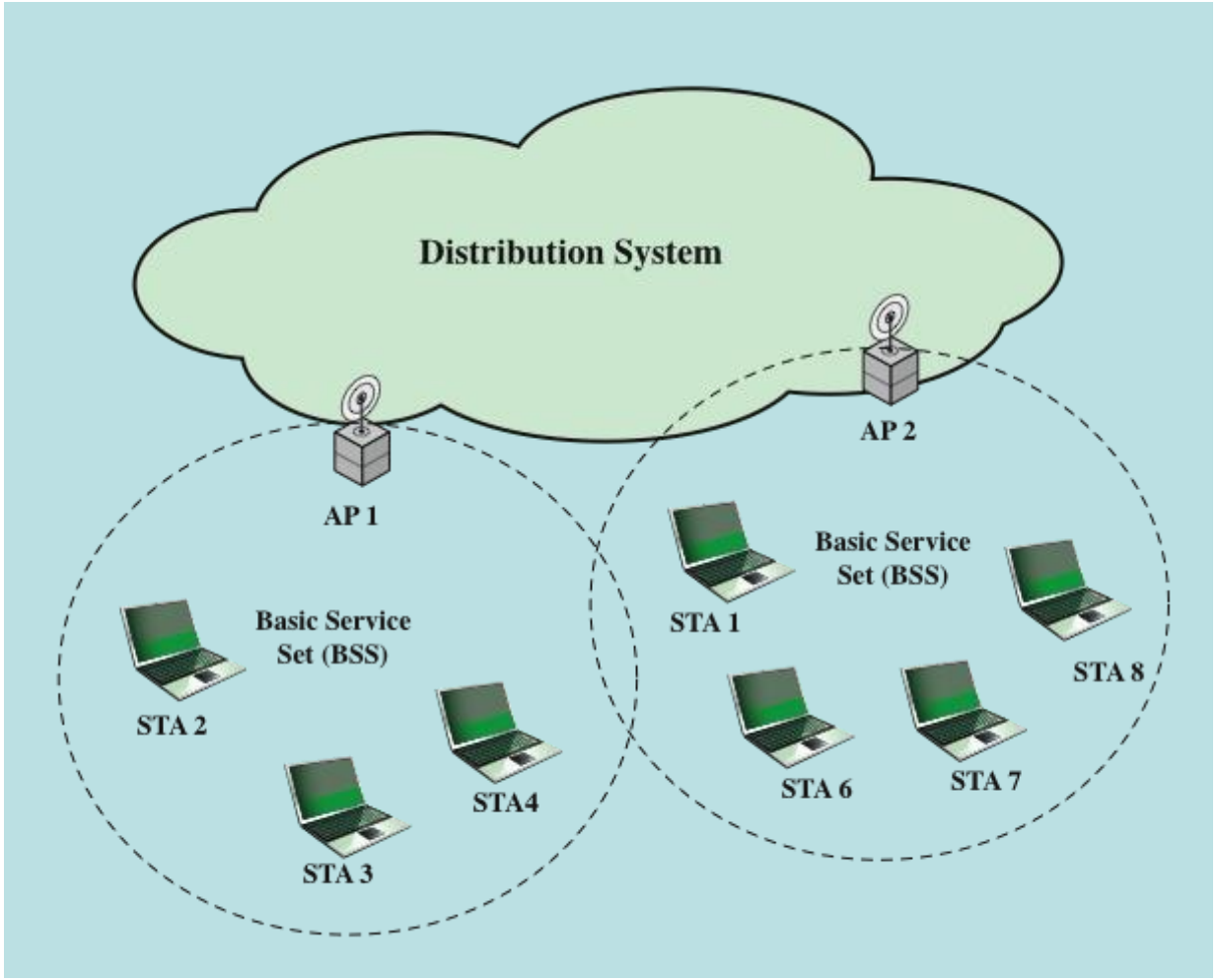
IEEE 802 Protocol Architecture



General IEEE 802 MPDU Format



IEEE 802.11 Architecture: Extended Service Set



IEEE 802.11 Services

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

MAC Service Data Unit (MSDU)

Service provider may be a station or DS; station services are implemented in every 802.11 station

Association Services

association

- establishes an initial association between a station and an AP

reassociation

- enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another

disassociation

- a notification from either a station or an AP that an existing association is terminated

Association-Related Services

- Transition types, based on mobility:
  - No transition
    - A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS
  - BSS transition
    - Station movement from one BSS to another BSS within the same ESS; delivery of data to the station requires that the addressing capability be able to recognize the new location of the station
  - ESS transition
    - Station movement from a BSS in one ESS to a BSS within another ESS; maintenance of upper-layer connections supported by 802.11 cannot be guaranteed

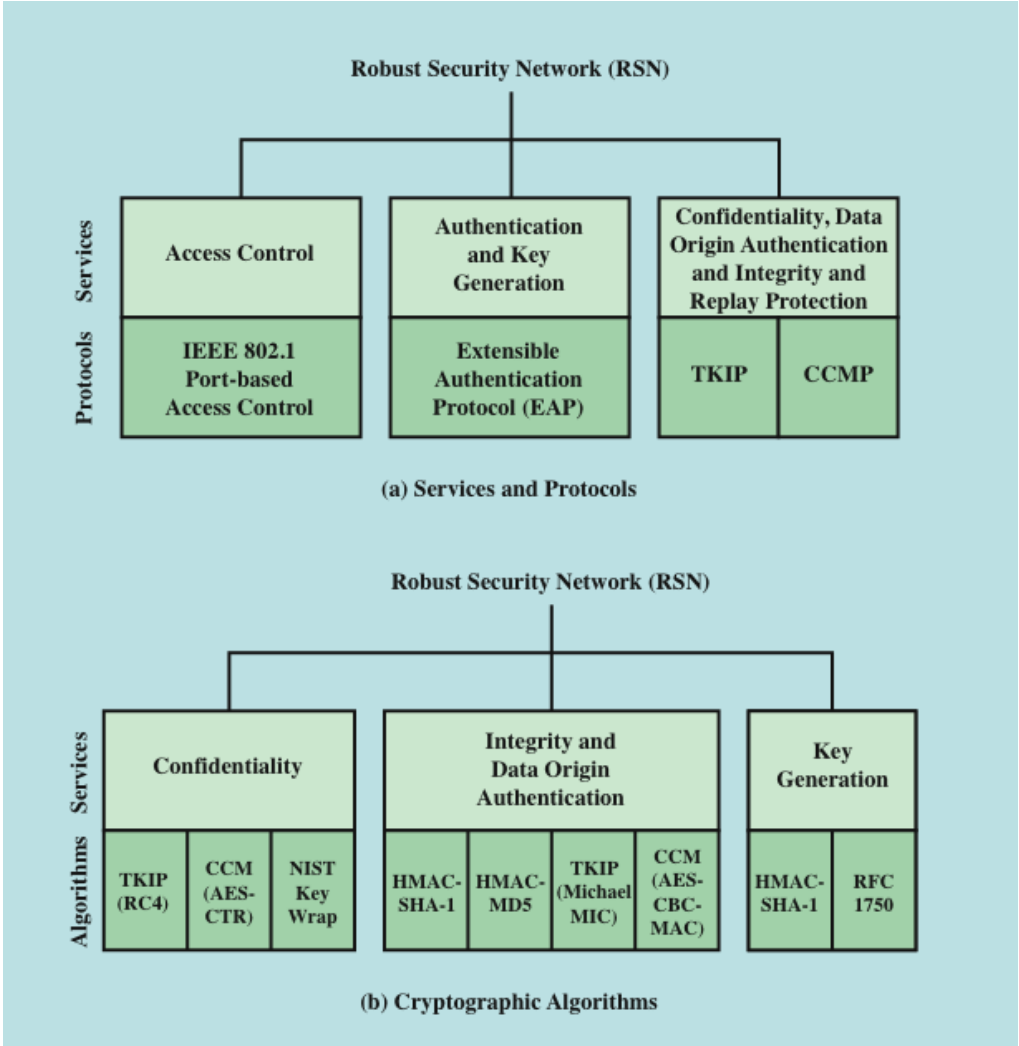
Wireless LAN Security Protocols

- Wired Equivalent Privacy (WEP) algorithm
  - 802.11 privacy
- Wi-Fi Protected Access (WPA)
  - Set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard
- Robust Security Network (RSN)
  - Final form of the 802.11i standard

IEEE 802.11i Services

- **Authentication**: the exchange between a user and an authentication server (AS); temporary keys are generated
- **Access control**: routes messages properly, facilitates key exchange
- **Privacy**: MAC level data are encrypted
- *Security protocols that support the above services: next page*

Elements of IEEE 802.11i

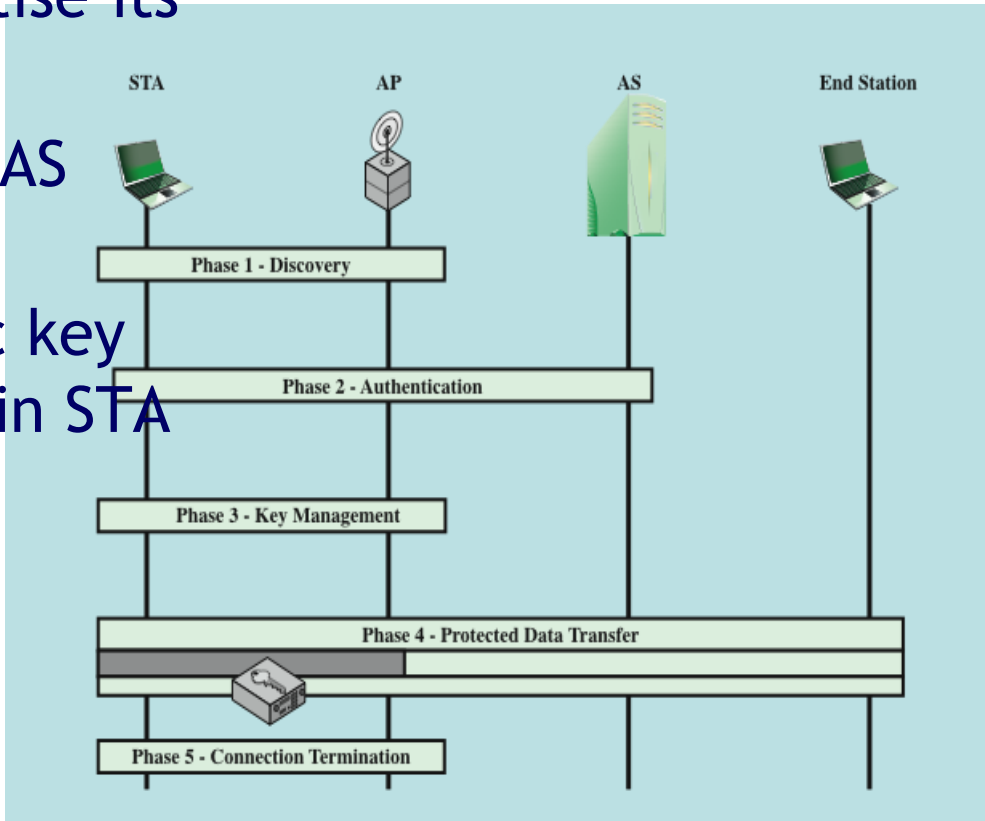


Phases of Operations: Possibilities

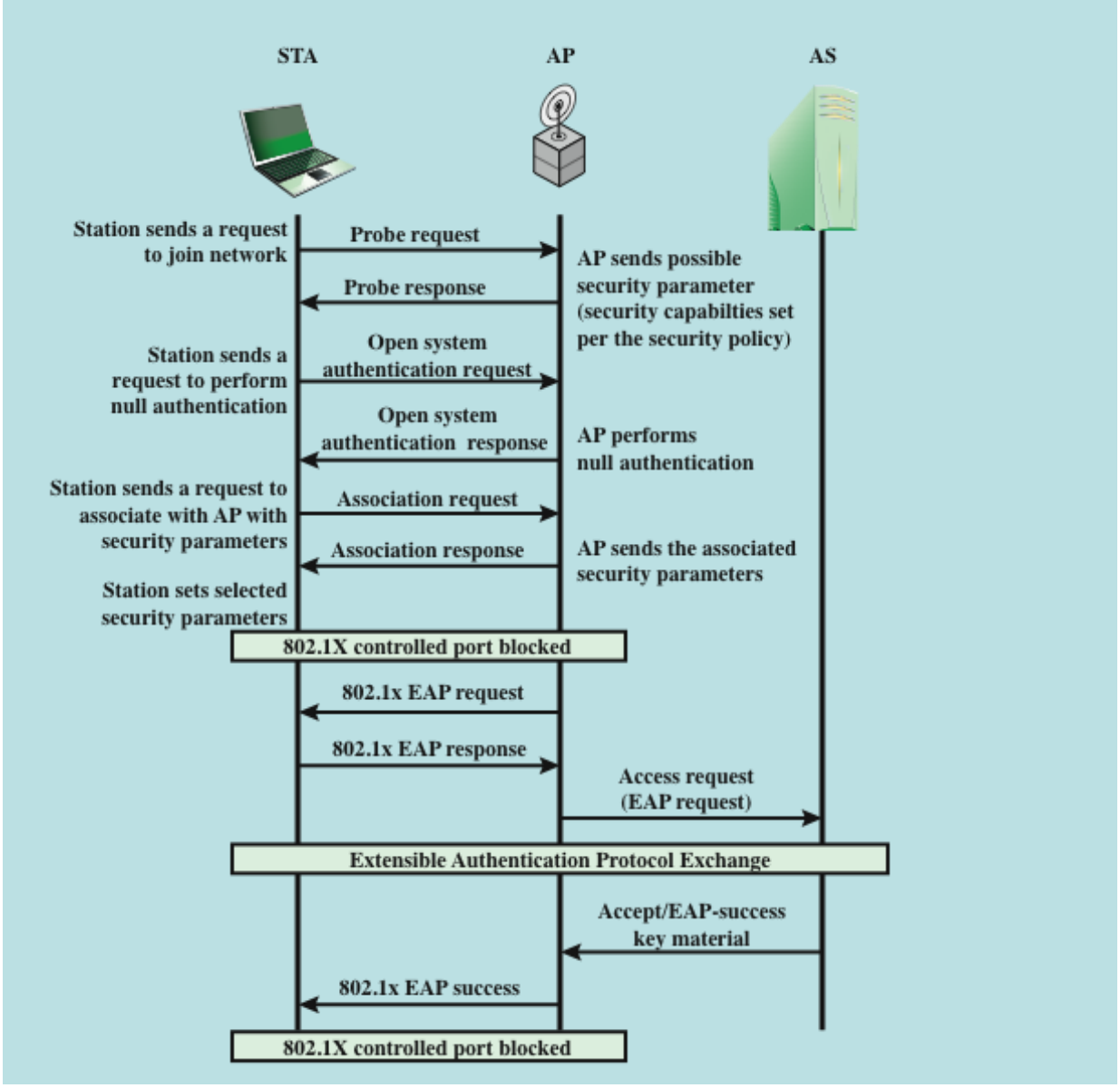
- Two wireless STAs in the same BSS communicate via an AP
- Two wireless STAs in the same ad hoc BSS communicating directly
- Two wireless STAs in different BSS communicating via their Aps
- A wireless less STA communicating with wired station via its AP

IEEE 802.11i Phases of Operation

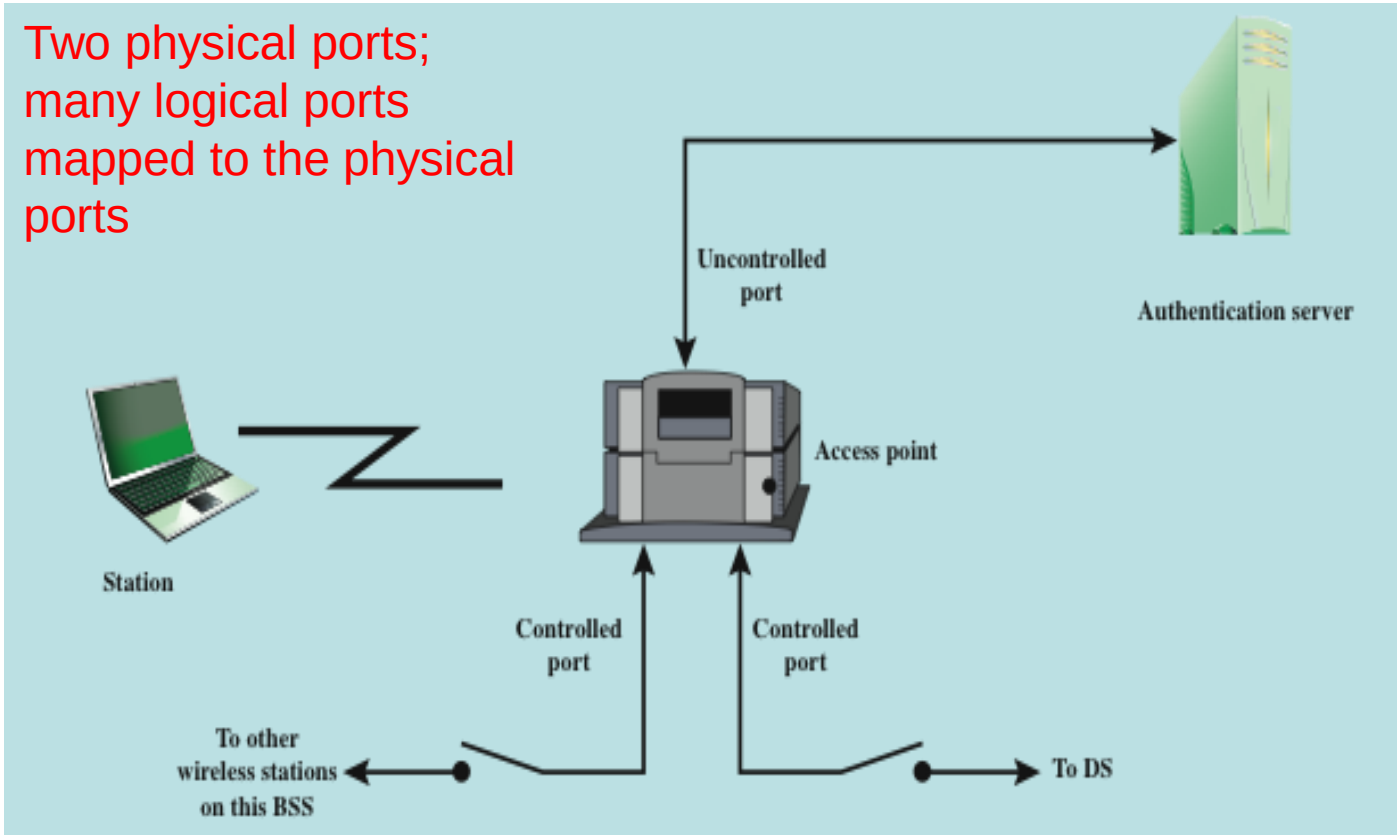
- **Discovery:** AP sends Beacon, Probe responses to advertise its 802.11 security policy
- **Authentication:** STA and AS prove their identities
- **Key MGMT:** cryptographic key are generated and saved in STA and SA
- **Protected data transfer**
- **Connection termination**



IEEE 802.11i Phases of Operation



IEEE 802.1x Access Control (for Controlling Access)



MPDU Exchange

- authentication phase consists of three phases:
  - connect to AS
    - the STA sends a request to its AP that it has an association with for connection to the AS; the AP acknowledges this request and sends an access request to the AS
  - EAP (Extensible Authentication Protocol) exchange
    - authenticates the STA and AS to each other
  - secure key delivery
    - once authentication is established, the AS generates a master session key and sends it to the STA

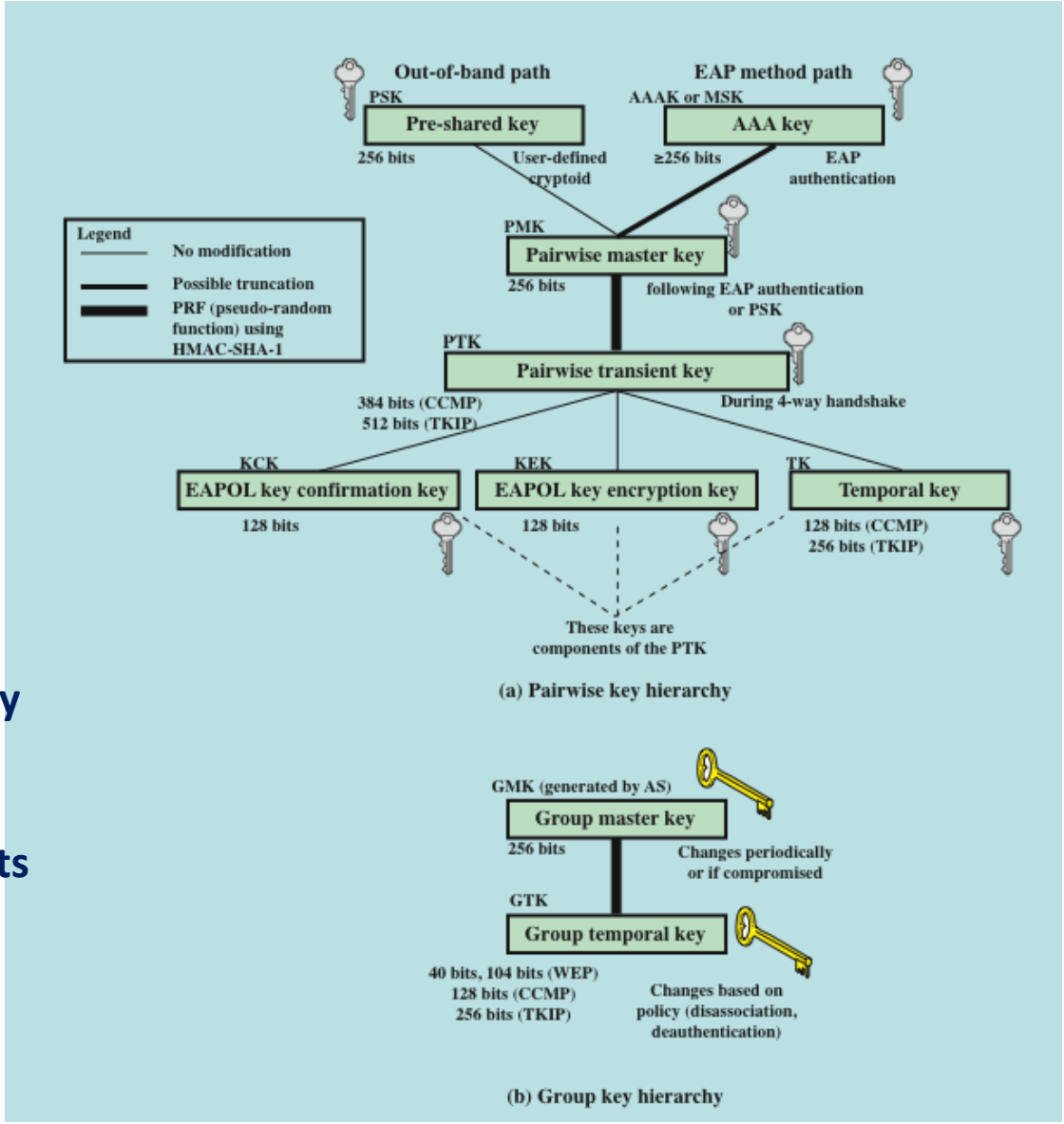
IEEE 802.11i Keys for Data Confidentiality and Integrity Protocols

EAP: Extensible Auth. Protocol

EAP over LAN: supports integrity and origin authentication

EAP Key Encryption Key: protects confidentiality

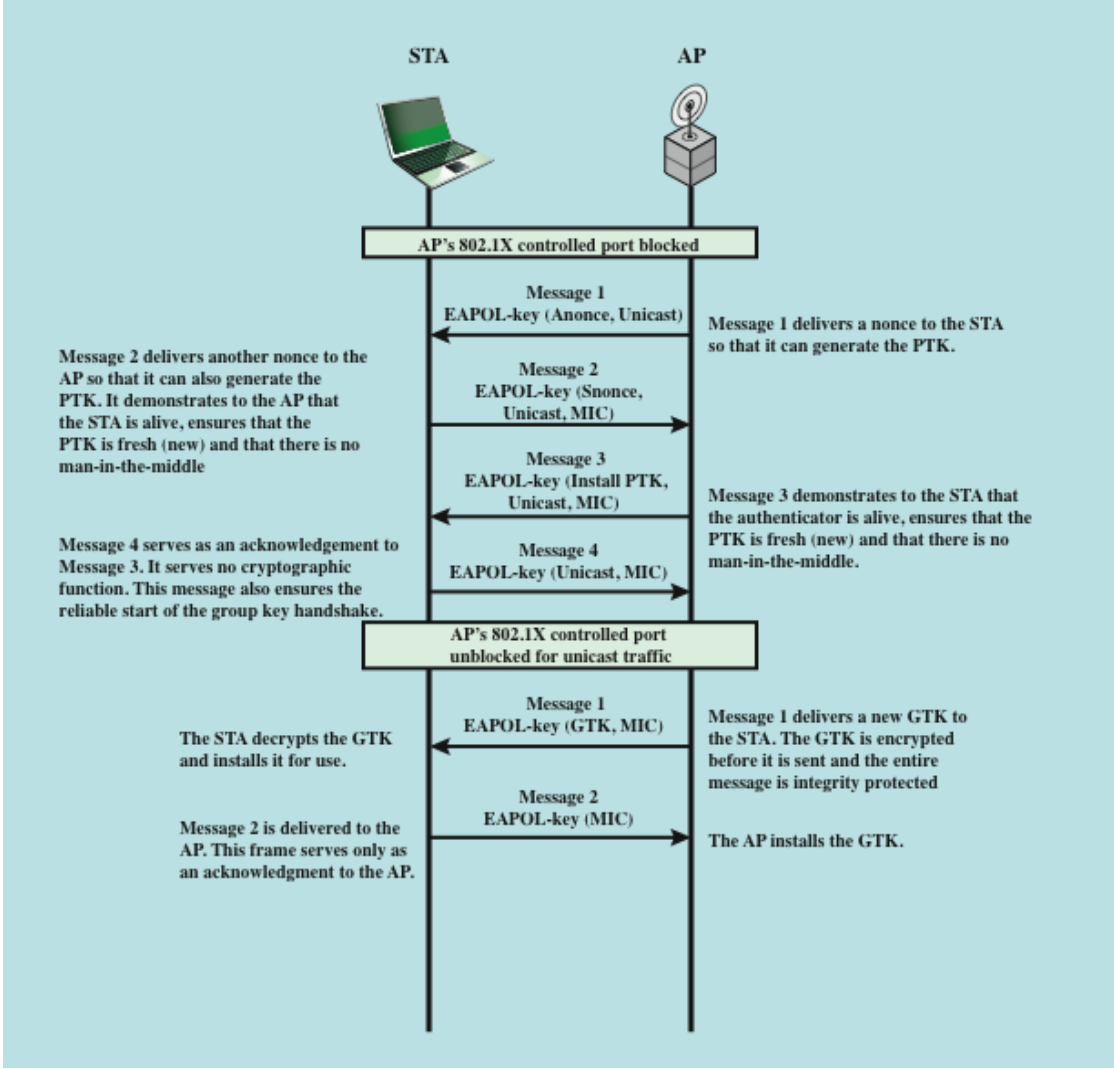
Temporal Key (TK): protects transmission



IEEE 802.11i Key Hierarchy (Key MGMT)

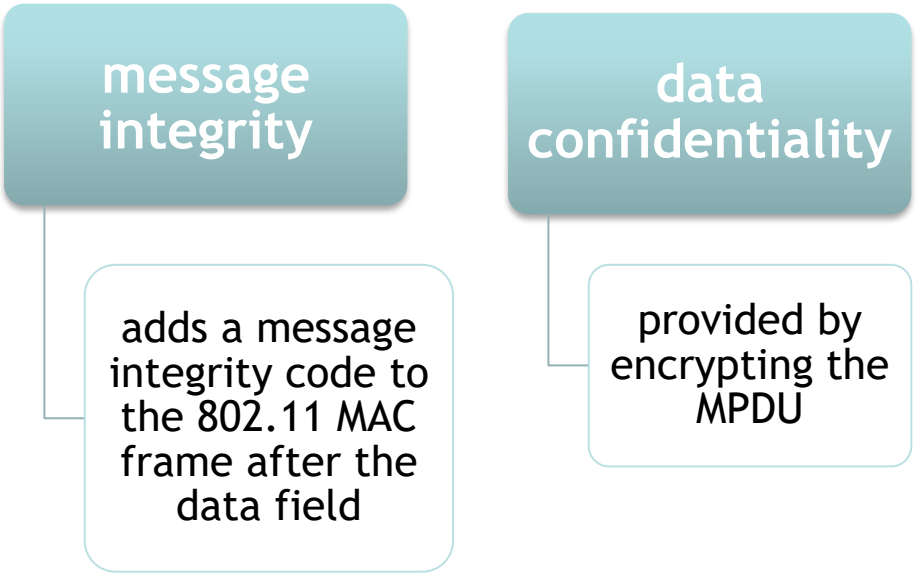
Abbrev-iation	Name	Description / Purpose	Size (bits)	Type
AAA Key	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MMSK.	≥ 256	Key generation key, root key
PSK	Pre-Shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
PMK	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pair-wise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic.	256 (TKIP) 128 (CCMP) 40, 104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40, 104	Traffic key

Phases of Operation: 4-way Handshake



Temporal Key Integrity Protocol (TKIP)

- Designed to require only software changes to devices that are implemented WEP
- Provides two services:



Summary

- Wireless security overview
  - wireless network threats
  - wireless security measure
- IEEE 802.11 wireless LAN overview
  - Wi-Fi alliance
  - IEEE 802 protocol architecture
  - IEEE 802.11 network components and architectural model
  - IEEE 802.11 services